DETAILED ACTION

Examiner's Amendment

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Richard Berg on December 15, 2008.

The application has been amended as follows:

In the claims:

54. [Currently Amended] A system according to ~~claim 53~~ claim 61, wherein said condition indicated in said encryption key is a condition that is to be met by particular data stored in the device and protected against subversion, the said authorised means being arranged to check this condition by reference to said particular data.

55. [Currently Amended] A system according to ~~claim 53~~ claim 61, wherein said condition indicated in the encryption key is a condition that is to be satisfied by input data presented by a user of the device, the device including input means for receiving said input data and the said authorised means being arranged to check the condition indicated in the encryption key by reference to said input data.

57. [Currently Amended] A system according to ~~claim 53~~ claim 61, in which the private key of the first key pair is securely stored in the storage means of the trusted authority entity, and said private data is securely stored in the storage means of the device.

58. [Currently Amended] A system according to ~~claim 53~~ claim 61, wherein said penultimate key pair is the second key pair in said chain, the trusted authority entity being arranged to provide the link between the start key pair and penultimate key pair by using the private key of the first key pair to certify said public data such as to indicate that an entity holding the corresponding private data is one to which it has delegated authority.

59. [Currently Amended] A system according to ~~claim 53~~ claim 61, wherein said authorised means is a key-generation process and a subversion-resistant operating environment for running said key-generation process.

61. [New] A system comprising:

a trusted authority entity including secure storage means for securely storing a private key of a first public/private key pair, and a device arranged to serve as a delegate for said trusted authority, the device including secure storage means; the system being arranged to host at least the private keys of a chain of public/private cryptographic key pairs that are linked in a subversion-resistant manner, this chain comprising:
a starting key pair formed by said first key pair, a penultimate key pair formed by public/private data; and an end key pair formed by an encryption/decryption key pair of an Identifier-Based Encryption, IBE, scheme; the secure storage means of the device being arranged to securely store said private data for access only by authorised means

pre-authorised by the trusted authority, the device further including said authorised means for linking said penultimate and end key pairs, said authorised means being arranged to provide said decryption key, generated using said private data and said IBE encryption key, only if at least one condition is satisfied, said at least one condition comprising a condition indicated in the encryption key.

Allowable Subject Matter

2. Claims 1-36 and 54-59 and 61are allowed.

3. The following is an examiner's statement of reasons for allowance: Applicant's arguments filed on 10/24/2008 in response to Non-Final office action mailed on 07/25/2008 are found to be persuasive. Claims rejections have been withdrawn.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

4. Any inquiry concerning this communication or earlier communications from the examiner should be directed to KARI L. SCHMIDT whose telephone number is (571) 270-1385. The examiner can normally be reached on Monday - Friday: 7:30am - 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on 571-272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Kari L Schmidt/
Examiner, Art Unit 2439

/Kambiz Zand/

Supervisory Patent Examiner, Art Unit 2434